BOLESTIC

Nº 3 Junio 2024

Boletín de concienciación en ciberseguridad

Esta comunicación está destinada a los profesionales públicos de la Administración

TITULARES

Consejos para unas vacaciones ciberseguras

Con la llegada del verano, la mayor parte de nosotros nos lanzamos a buscar dónde pasarlas, navegando en webs de alquileres vacacionales y a la caza de la mejor oferta o chollo.

Pág. 2

Lo que la ciberseguridad corporativa debe aprender del fútbol

La ciberseguridad y el fútbol tienen más cosas en común de lo que puede parecer a priori. Los equipos de fútbol deben planificar sus partidos dependiendo del rival y del juego. Lo mismo ocurre con las empresas, que viven en un contexto de ciberataques cada vez más complejos.

Pág. 3

Ataques a las contraseñas

Conocer cuáles son las estrategias que usan los ciberdelincuentes para intentar robar contraseñas nos ayuda a protegernos mejor de posibles ataques y amenazas.

Pág. 4

Un año más, Digital Enterprise Show

Este mes de junio Málaga acogió Digital Enterprise Show (DES - Show), un evento que convirtió a la ciudad en el epicentro de la innovación digital, impulsando la identificación y creación de oportunidades empresariales y profesionales.

Este año bajo el lema «feel the exponential intelligence», el Congreso contó con más de 450 expertos internacionales y multitud de actividades.

La Agencia Digital de Andalucía participó de forma activa en el encuentro, tanto en la agenda general con charlas y mesas debate como en la zona expositiva, en la que se ubicó un amplio stand con espacio para charlas, networking, pantallas interactivas y mucho más, poniendo a las personas en el centro de la tecnología.

Vídeo del evento

DE INTERÉS

Curso de Seguridad en dispositivos móviles iOS (Online y gratuito).

Más información aquí.

El POST-IT

Acceso a equipamiento, aplicaciones y sistemas

LA PELÍCULA

CONTRAPORTADA

Comprueba si tu cuenta de correo está comprometida, https://haveibeenpwned.com/. Si es así, **cambia la contraseña**.

BOLESTIC
Nº 3 Junio 2024
Boletín de concienciación en ciberseguridad
Esta comunicación está destinada a los profesionales públicos de la Administración

TITULARES

Consejos para unas vacaciones ciberseguras

Con la llegada del verano y las tan deseadas vacaciones, la mayor parte de los usuarios se lanza a buscar dónde pasarlas, navegando en webs de alquileres vacacionales y a la caza de la mejor oferta o chollo. Sabemos que las vacaciones están para disfrutar y por eso, te facilitamos recursos con los que aprender a detectar posibles fraudes durante estos días de desconexión. Sin embargo, las amenazas son muchas y no podemos ignorarlas. Así que, sigue estas sencillas pautas para proteger tu privacidad y hacer de tus vacaciones, unas vacaciones ciberseguras.

Presta atención a los fraudes. En verano, la demanda de alquiler de viviendas por vacaciones se multiplica y también lo hacen los fraudes.

Ten cuidado con los correos. En vacaciones, los intentos de phishing y los ataques de ingeniería social aumentan.

Pon a punto tus contraseñas. Es un buen momento actualizar tus contraseñas, o al menos, aquellas que protejan la información más sensible antes de irte unos días de vacaciones.

Haz copias de seguridad. Seguro que durante tus vacaciones sacas muchas más fotos de lo habitual y es posible que te quedes sin espacio en tus dispositivos.

Cifra tu información. El cifrado de tus dispositivos es muy útil si por un descuido acabas perdiéndolos, extraviándolos o si fuesen robados.

No compartas toda tu vida en las redes. Tu privacidad es más importante que ganar unos cuantos likes. Una fotografía o vídeo puede revelar mucha más información de lo que crees.

Mucho ojo con las redes públicas. Las wifi públicas son como un estanque de peces donde no sabes si puede haber algún tiburón acechando. Así que, si vas a conectarte a una, lo mejor que puedes hacer es minimizar los riesgos:

- No accedas a ninguna cuenta personal (redes sociales, correo electrónico, tienda online).
- No introduzcas datos sensibles, como el número de tu tarjeta de crédito.
- Navega mediante el modo incógnito.
- Utiliza una VPN.

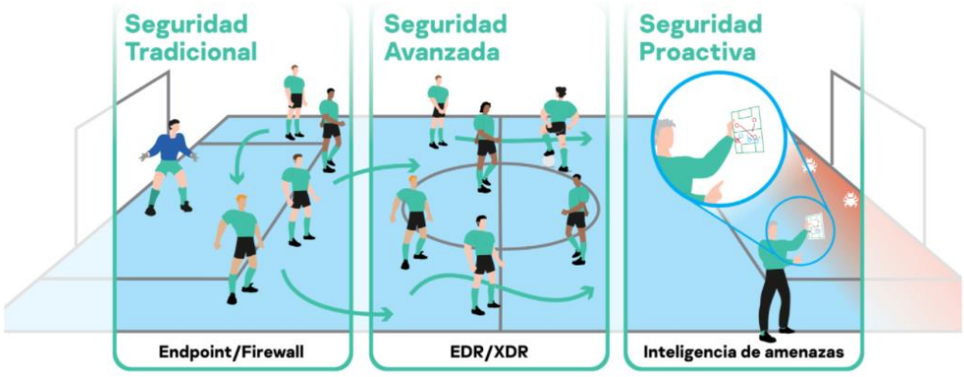
Cuidado con las apps de moda. Otro tipo de amenaza en auge durante las vacaciones son las apps de moda, especialmente aquellas relacionadas con las fotografías o de tipo social.

BOLESTIC
Nº 3 Junio 2024
Boletín de concienciación en ciberseguridad
Esta comunicación está destinada a los profesionales públicos de la Administración

Lo que la ciberseguridad corporativa debe aprender del fútbol

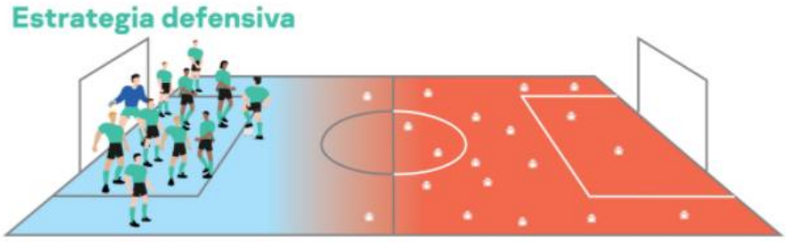
Replegarse para adoptar una posición defensiva en fútbol puede tener inconvenientes. Lo mismo ocurre en entornos empresariales cuando se trata de ciberseguridad.

Otra similitud entre el fútbol y la ciberseguridad empresarial es la forma en la que cada equipo y compañía deciden "jugar". Puedes jugar a presionar alto o poner el "autobús" en tu portería y esperar que no te metan gol.



¿Encerrarse atrás es la mejor estrategia?

Aunque una postura defensiva pueda parecer una estrategia ideal, esa decisión pueda dejar vulnerables tanto al equipo como a la empresa y no brinda el tiempo necesario para reaccionar ante una amenaza.



Puntos positivos:
- Sensación de seguridad
- Concentrarse en no perder

Puntos negativos:
- Los adversarios aprovechan los puntos débiles
- No hay tiempo para reaccionar ante un ataque
- Sólo puedes ver el ataque cuando está en el área de defensa (endpoint/firewall)

Una defensa proactiva

La primera línea de defensa de cualquier empresa será el famoso antivirus y el firewall -y aquí ya incluye la protección en entornos de nube y el EDR-. Todos son básicamente reactivos, ya que solo se activan cuando los ordenadores o servidores son atacados, y es solo en ese escenario donde se sabrá si funcionan bien o no.

Estrategia proactiva

Puntos positivos:
- Anticipa la identificación de los ataques
- Posibilidad de bloqueo en diferentes momentos (más protección)
- Puede ver el ataque desde su origen (a través de endpoint, red, accesos + datos de campo extras con Threat Intelligence)

Puntos negativos:
- 1. Requiere que la empresa tenga un equipo de seguridad interno o externo

BOLESTIC
Nº 3 Junio 2024
Boletín de concienciación en ciberseguridad
Esta comunicación está destinada a los profesionales públicos de la Administración

Ataques a las contraseñas

¿Qué tipos de ataques existen?

Fuerza bruta

Consiste en adivinar la contraseña a base de ensayo y error.
Los ciberdelincuentes prueban distintas combinaciones al azar, conjugando nombres, letras y números, hasta que dan con el patrón correcto.

Ataques de diccionario

Un software se encarga automáticamente de intentar obtener la contraseña.
Empiezan con letras simples como "a", "AA" o "AAA" y, progresivamente, va probando con palabras más complejas.

Phishing

Una de las técnicas más utilizadas por los cibercriminales para robar contraseñas y nombres de usuario.
Se engaña a la víctima para que rellene un formulario fraudulento que suplanta a un servicio con sus credenciales de inicio de sesión.

Ataque keylogger

La víctima instala el malware en su equipo al hacer clic en un enlace o descargar un archivo de Internet.
Una vez instalado, el keylogger captura todas las pulsaciones del teclado, incluyendo las contraseñas, y se las envía a los ciberdelincuentes.

¿Cómo proteger nuestras contraseñas de estos ataques?

Contraseñas complejas

Utilizar más de 8 caracteres incluyendo mayúsculas, minúsculas, números y caracteres especiales.

Contraseñas diferentes

No reutilizar contraseñas, usa contraseñas diferentes para distintos servicios.

Cambiar con regularidad

Dependiendo de la criticidad de la información que maneje el servicio, se establecerá una mayor o menor periodicidad para el cambio de contraseña.

Pero ¿qué es la ingeniería social?

La ingeniería social es muy utilizada por los ciberdelincuentes y se trata de técnicas de engaño y manipulación para hacerse con los datos de los usuarios. Toma nota de los siguientes consejos para no caer en trampas:

No reveles nunca información personal ni datos confidenciales (credenciales, números de tarjetas de créditos, cuentas bancarias, etc.) por teléfono, email o redes sociales, podrían estar suplantando la identidad de alguna empresa o servicio.

Ten cuidado al compartir información. Evita exponerte en Internet y en redes sociales publicando información personal (número de teléfono, dirección, hábitos, etc.). Éstos facilitan el trabajo a los ciberdelincuentes, si quieren, por ejemplo, adivinar tu contraseña.

Verifica los ficheros adjuntos y enlaces. No los descargues ni accedas a ellos si desconoces su contenido, aunque provengan de un contacto conocido, podrían tratarse de un Keylogger u otro malware.

Utiliza el sentido común y recuerda que en Internet el mejor sistema de seguridad eres tú

OSI Oficina de Seguridad del Internauta

BOLESTIC
Nº 3 Junio 2024
Boletín de concienciación en ciberseguridad
Esta comunicación está destinada a los profesionales públicos de la Administración

EL POST-IT

Acceso a equipamiento, aplicaciones y sistemas

Código de conducta en el uso de las tecnologías de la información y la comunicación para profesionales públicos de la administración de la Junta de Andalucía.

Los profesionales utilizarán los mecanismos de acceso implantados para el equipamiento, las aplicaciones y los sistemas.de Andalucía.

Se custodiarán diligentemente sus credenciales de acceso, sin proceder a su revelación o puesta al alcance de terceros. Serán responsables de toda la actividad realizada con sus credenciales.

Si sospechan que sus credenciales de acceso están siendo utilizadas por otra persona, procederán inmediatamente a su cambio y notificarán la correspondiente incidencia de seguridad.

Nunca se intentará obtener, por medios ilícitos, derechos de acceso superiores a los que les correspondan, ni utilizar las credenciales de otras personas.

Cumple con las obligaciones de secreto y confidencialidad, y por supuesto con la normativa vigente en protección de datos.

BOLESTIC
Nº 3 Junio 2024
Boletín de concienciación en ciberseguridad
Esta comunicación está destinada a los profesionales públicos de la Administración

LA PELÍCULA

Mejor sonreir que llorar

Vivimos rodeados de tecnología de información y de comunicaciones (TIC) en todos los ámbitos, tanto en el profesional, como en el personal.

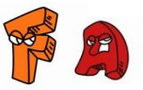
El uso seguro de estos medios puede ser la diferencia clave entre nuestras sonrisas y nuestras lágrimas.

Las 8 notas musicales


sifica la información que publicas en redes sociales.


cuerda que la seguridad TIC es cosas de todos, de ti también.


nimiza los riesgos (web falsas, correos de emisores desconocidos, etc).


miliarízate con el uso seguro de los medios.


icita ayuda a tu CAU ante cualquier incidente o problema.


contraseña, no la reveles a nadie.


tienes consultas o dudas sobre seguridad escribe al CAU o la Unidad de Seguridad TIC de tu Consejería y serás atendi 

BOLESTIC
Nº 3 Junio 2024
Boletín de concienciación en ciberseguridad
Esta comunicación está destinada a los profesionales públicos de la Administración

CONTRAPORTADA

Cada cuánto hay que apagar y encender el móvil y qué ventajas de seguridad ofrece hacerlo

No se trata de reiniciar el móvil, sino de apagarlo por completo y después volver a encenderlo. Para más información, pulsa aquí.

Wangiri: la peligrosa estafa del "llama y cuelga"

Regresa una de las estafas más conocidas por todos, pero ahora en versión 2.0 y amparada en la inteligencia artificial, multiplicando así su peligro. Para más información, pulsa aquí.

Del chip del perro al marcapasos: dispositivos que jamás hubieses imaginado que te puedan piratear

Al pensar en hackeos, mucha gente tiene presentes su ordenador o su teléfono móvil. Pero en realidad existen muchos otros dispositivos vulnerables... y cada vez más. Para más información, pulsa aquí.

Un desconocido me escribe en WhatsApp: qué debes hacer, cómo comprobar si es una estafa y qué hacer si lo es

Entre filtraciones y despistes, es muy posible que muchos de nuestros números de teléfono estén siendo filtrados por la red. Esto se traduce en que puedes recibir mensajes de desconocidos. Para más información, pulsa aquí.